IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 9, Issue 3 (May. – June. 2022), PP 01-12
www.iosrjournals.org

TITLE

Cyber First-Aid

Olebara Comfort Chinaza
Department of Computer Science, Faculty of Physical Science, Imo State University, Owerri, Imo State, Nigeria.

Abstract
The role of research in national development cannot be over-emphasized. Research is the act of proffering solution(s) for present and future problems through knowledge contribution, seeking, and organization. The ability for one to find old or new knowledge or generate new ones, as well as follow a set of knowledge organization rules towards answering research question(s) makes him/her, a researcher. The process and set of activities followed by the researcher has in recent times, involve knowledge exchange, collaboration and blending, mostly through digital media, with the cloud as the main storage and linked via several, wired, wireless, hardware, and software interfaces. The described system is prone to cyber-attack and must be protected, as most researches are funded by interested bodies and their outcomes highly evident in national development. This work christened "Cyber First-Aid" is geared towards creating situational awareness on the need for researchers to protect their finished or on-going intellectual property from hackers. The methods proposed are not be best-practices in the cyber security domain but easily applicable checks and solutions with Graphical User Interface applications that any researcher with minimal computer knowledge can implement in order to increase cyber hygiene and minimize intellectual property loss. Protocol analyzers, packet capturers, hash key generator, and Virus Total malware search engine are some of the programs that are required in researchers' cyber First-Aid tool box. These tools have Graphical User Interface (GUI) hence they can be easily used by researchers with minimal computer knowledge. The result is a security-conscious researcher who implements measures required to safeguard his system, intellectual property, and associated data from malicious attacks.

Keywords: *Cyber security, Malware, Security, First Aid, Intellectual property, Protocol, Network, Packet, Researcher.*

Date of Submission: 20-25-2022 Date of Acceptance: 03-06-2022

I. Introduction

Research and Development in the era of IoT can be termed a Sustainable disruptive Technology. This assertion follows the many technological developments geared towards enhancing R and D processes and bringing knowledge engine closer to researchers. "Things" in the world of research include: learning (remote learning), simulation of real experiments, search engines, browsers, cloud services, internet resources, service providers under the "aaS" (as a Service) tech-word. Example: Software as a Service (SaaS), Security as a Service (SaaS), Cloud as a Service (CaaS) etcetera. Before the internet and its associated "WWW" (world wide web), undergraduates, post graduates, and researchers from all fields of study and/or interest domains spend tons of time in physical libraries, scanning through volumes of dusty textbooks, which in most cases, were obsolete, as many libraries especially in developing countries could not afford updated and current versions. The advent on internet changed the narratives by presenting quality and up-to-date content, brought about collaborative research among scholars across disciplines and nations, and reduced the digital gap between developed and developing nations. As a result of the foregoing, the quality of R and D has improved, with many nations and organizations providing huge grants for the funding of projects of interest. [1] found an increase in the number of countries engaging in research grants and the size of the grants. [2] investigated the effects public funding has on the funded sectors, and found that a positive relationship exists between research funding and collaborative innovation, and that innovative output is enhanced when research is funded. [3] studied the impact funding has on collaborative scientific research and found that a positive and statistically significant relationship exists between funding and collaborative research as reflected in the increased number co-authors in peer reviewed paper. Secondly, the authors found an extended ego network and the indirect and co-opted authors. This means that the network formed by the lead author termed "ego" and co-authors termed "alters" is larger in funded projects and that a second tier exists where these authors bring in support-authors where necessary, so as to successfully accomplish the task. In quantifying the economic impact government and charity funding of

medical research on private R and D funding, a statistically positive association was found between public biomedical, health research expenditure, and private research and development in the pharmaceuticals [4]. The impact of research outcome in the health sector is evident in the recent COVID-19 pandemic that brought about the death of many, and had nation's leaders observe lock-down policies to restrict movement and limit its spread. Heavy investments in research have today yield a favorable sustainable outcome through vaccine for the various variants of the pandemic. Researchers from all disciplines can be said to be the high consumers and contributors of online content, which in turn makes them vulnerable to cyber-attacks or self-acquired malware in their line of duty which includes: intellectual-property development, knowledge extraction and sharing, use and reuse of data, technological advancements through reverse engineering, teachers and learners without borders, etcetera. It also has adversarial effects of increased cyber-attack majorly to steal intellectual property and intelligence [5].

Definition of some of the cyber security key words as guide to non-Computer science researchers who would adopt the cyber First-Aid.

-Cyber is used to describe computers networks and their cloud storage. Example is the internet [6].

-Cyber space is a global container in the information system related networks, their infrastructures, information systems, computer system, and other embedded semiconductor units, Internet, telecommunications networks, computer systems, and embedded processors and controllers [7].

-Cyber-attack is an attack carried out on any information or information technology that operates in cyber space. [8] defined it as an attack in cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

-Cyber security is the practice of shielding information and information technologies from cyber-attacks, as well as helping them overcome a successful attack. [9] listed the technologies that make up the information technology in his definition of Cyber security as the practice of defending networks, data, servers, computer and mobile devices from malicious attacks.

[10] presented 15 cybersecurity statistics in the education sector, which agrees with the findings of [5], that intellectual property and intelligence are the major targets for cyber- attack.

The paper is organized as follows: Section 1 introduces the motivation behind the paper such as the and role importance of research and development in nations' and organizations' economy through sustainable disruptive technology such as the internet as well as underscores the success of research outcomes in many sectors. Section 2 reviews related literature through conceptual framework, review of malware attacks and attack vectors review of network analysis methods for malware detection and containment. Section 3 presents material ands and methods for malware investigation, while section 4 draws conclusion and makes recommendations through an outline of proposed methods.

II. Literature Review

A. Conceptual Framework

Computer network is a collection of multiple computers, that can share peripheral, software, internet connection and applications and connected using a wireless or wired media. The internet is a wider network, with interconnection of millions of computers and electrical device across the globe, linked through a TCP/IP Protocol. The internet is also known as network of networks [11]. According to [12], data related to network security measurement can be divided into four categories namely: packet level, flow-level, connection-level, and Host-level. In computer networking, data transmitted over a network is divided into smaller units called packets. The packets travel through the transport protocols and are collated by the receiving computer into its original form (data) [13]. Network flow data are digital records such as source and destination addresses, source and destination port numbers, protocols, timestamps that make up the connections. describe and characterize connections made over a network, including data elements such as IP addresses and port numbers for source and destination endpoints, protocols, traffic volume, timestamps, and network interfaces utilized, but without the content itself. Connection-level data are generated during HTTP/TCP connection. [12] observed that packets are generated when Transmission Control Protocol (TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) as well as other related protocols, are run over a network. Features of packet data are: header information, payload information, activity information. Many software libraries for monitoring, analyzing and capturing data exists. These tools may be used by the hacker and victim alike: by the hacker to monitor victim's frequently visited sites and URLs of interest, and develop a similar compromised one, by the victim to monitor and analyze his/her network as well as scan for malware.

B. Malware Attacks and Attack Vectors

[14] describes malware related payload as trojan, virus or worm, that is used to carry out malicious attack on victim's computer. Malware's action on the target computer, such as theft of confidential information,

compromising data integrity, keylogging, or phishing activities and even data or computer system damage. The reliability of data collection method directly influences the integrity of the collected data. The internet has been proved to be a valuable tool in the researcher's tool box, hence internet data repositories, sources, and their destination in the researcher's computer, as well as other associated links, must be secured. Erman et al [15] presented a pictorial view of a Distributed Denial of Service (DDoS) attack (Fig.1).

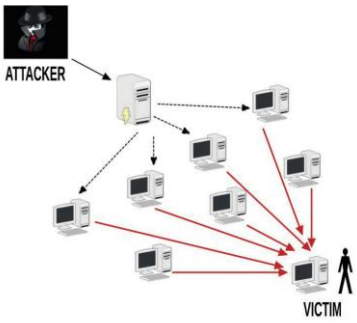


Fig 1. DDoS Attack. Source: [15]

The figure shows the attacker with his network of methods, connections, and attack vectors aimed at a victim's computer. For [15], monitoring network traffic with packet sniffers reveal the packets that flow in and out of a computer. These packets can be captured using packet capturers, and analyzed for malware. [16] proposed a framework that allows data trustworthiness assessed by: how free from error and up-to-date the data is, as well as how reputable its source is.

Attack Vectors

The hacker has many attack patterns which are termed attack vectors. [17] analyzed cyber-attack vectors and outlined the available attacks as:

-Compromised Employee: An employee who is a member of an organization's network may have his device compromised. This may in turn compromised any network to which the device is connected.

-Phishing e-mail attacks: e-mails masked as bank statements or any interest area the hacker observes the victim has interest may be used to lure a victim into allowing keyloggers or other payloads.

-Third party systems: web servers allow download of applications, PDF files, video steaming, pictures, etc. any on which may contain malware.

-Removable media: External storage devices, cameras with their memory cards are vulnerability sources

-Mobile device attacks or targeted network attack: a particular user's device or a particular network of interest may be targeted for an attack.

C. Network Analysis for Malware Detection and Containment

Many approaches and tools have been proposed for capturing required data segments from a life network, exporting and saving the file in dataset formats, analyzing the data, malware detection and blocking the source of attack. [18] proposed a protocol that allows resources to be shared using different packet switches networks. The protocol manages variation in individual network packets, offer flow control, manage transmission failures, sequencing, flow control, end-to-end error checking, as well as creation and destruction of logical processes. [19] proposed classification of contents that identify executable contents in incoming packets. Their two-step method first analyzes the packet payload for the presence of multimedia datatype such as avi, wmv, jpg, otherwise the payload is classified as text datatype such as txt, jsp, asp, or as executable such as .exe. [14], [20], [21] and [22] proposed various machine and deep learning approaches to malware detection. [23] proposed an interesting machine learning approach for detection of cyber -attack deployed on PDF files. The learning-based PDF malware detection method first converts PDF file to grayscale images, extract the image features, before applying machine learning for malware detection. Other peer-reviewed detection methods were focused on detecting malware by using the network data to carry out a sequence of activities geared towards packet capturing, malware detection, and source flagging/isolation. [24] proposed Network Traffic Analysis by detecting web-server (HTTPs) based malware. Similarly, [25] proposed deep packet analysis for DDoS attack detection. [26] also focused on network analysis, extraction of behavioral features across different protocols and work layers, employed feature selection for prioritizing the features, and finally applying various supervised learning algorithms to detect and attribute malware.

Use of hash key generation for malware detection is a common malware detection method, with many freely available GUI hash key generators that provide a match for the particular malware present in the file.

[27] refers to the hashing function as a fingerprint for malware. [28] reviewed many hashing algorithms, highlighting their strengths and weaknesses with respect to malware detection. [29]presented a methodology for malicious file hash detection. This is displayed in Figure 2 below:

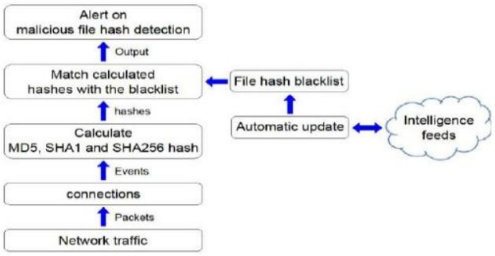


Fig.2 Methodology for malicious file hashing. Source: [29]

III. Materials and Methods

A. Purpose of the Study

Many researchers see the recommended computer security practices recommended in most beginners' textbooks and peer reviewed works such as [30] and [31], as exercise meant only for Computer science professionals or IT personnel, hence they get on with their computers, with pre-installed antivirus (for new laptops). This too soon expires and may never get replaced. The middle-class researchers settle for fairly-used computers and not many of this category understand need for security. This study is not aimed at unravelling the impact of R & D or its funding, but to draw attention to the massive interest in R & D in recent years, which is reflective in the increased grant value and funding bodies, create situational awareness of the researchers' vulnerability, and propose a methodology christened "cyber First-Aid" which is a diagnostic sequence of activities, mostly in Graphical user interface (GUI) environments, that will help a researcher secure intellectual property.

B. Research Questions

1. Which are the infected files and their hashes?
2. What is infected files' Domain name?

C. Materials

The table below lists tools required in the researchers' cyber First-Aid box and their functions. These are not best-practices in computer or cyber security, but considers factors such as: Ease of use, measured by how easy it is to learn the technologies presented, fewer number of clicks, easy to remember steps are, considering that the target group (researchers) are from various study fields and have varying degrees of digital know-how.

Table 1: Cyber First-Aid Toolbox

S/N	Tool	Example	Tool Application
1.	Packet Sniffers/analyzers	TCPDUMP, Wireshark https://www.wireshark.org/download.html	Computer application used to intercept network traffic, get details of dataflow, their sources and destinations as well as data items they convey.
2.	Key Hashing program	Hashmyfile.exe	Computer program used to extract the MAC address of applications captured by packet sniffers
3	Virus Detection program	Virustotal.com/gui/home/search	Website that analyzes URL, IP addresses, files and domains to find malware and breaches
4.	Anti-Virus	Norton, Kaspersky	Software for system protection
5.	Clearing browsing history		
6.	Cyber hygiene best-practices		

D. Methods

Steps to Researchers' Cyber First-Aid: Computer Security Best Practices should be observed at all times. These include:

1. Researchers engage in basic cyber hygiene practices such as:

i. Having up-to-date antivirus

ii. Ensuring the system firewall is on
iii. Scanning the computer with active antivirus from time to time
iv. Verifying URL publishers before downloading from them
v. Not opening e-mails you are not sure of.
vi. Backing-up files to the cloud is also recommended.
vii. Keeping system and application software up-to-date

2. Clearing browsing cache

Browsers save website information such as sites visited, downloads, files used to run online applications, in their cache memory as well as in cookies. Clearing browser cache protects personal information that may have been stored by the browser and cookies. To clear cache (Chrome):
-click three dots top right of Chrome browser -> More tools -> clear browsing data -> clear data

3. Malware analysis of packets, e-mail and files.

i. Download and install Wireshark version 3.6.3 that is appropriate for your operating system from the URL in table 1.

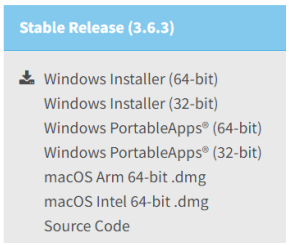


Fig. 3: Operating system options Source: [32]

ii. For packet data capturing, launch wireshark application as an admin (right-click on the application and select run as admin.

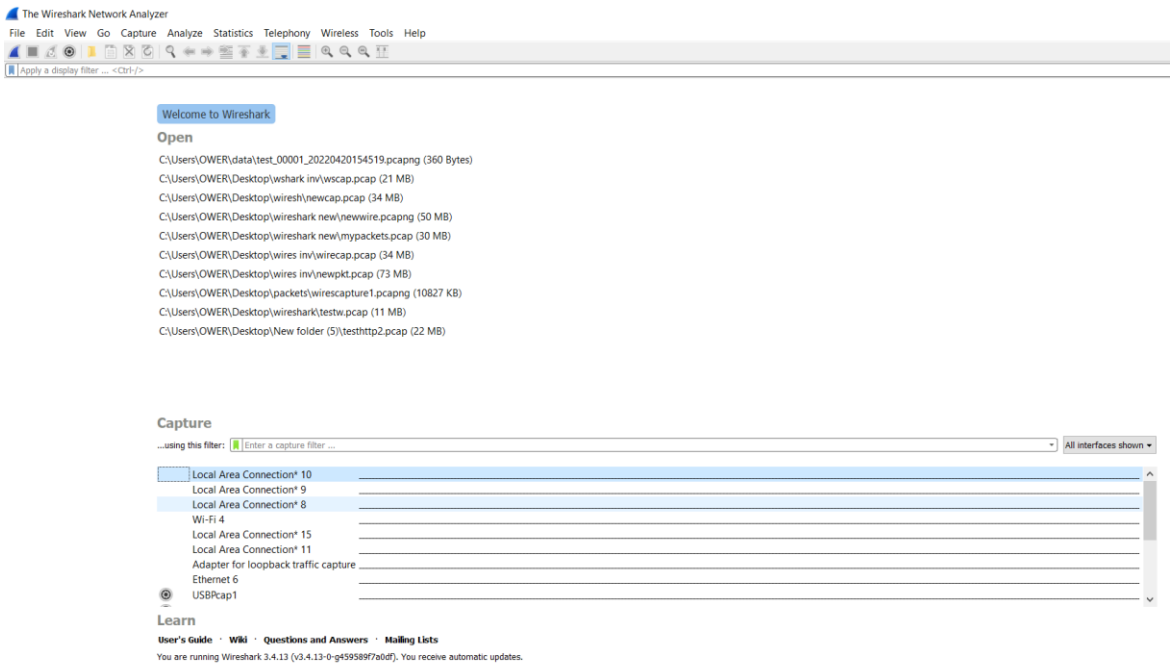


Fig. 4: Capturable connections

On launching Wireshark the window above (fig 4) is displayed. Fourth button under file menu allows you to set capturing options such as:
Input: show capturable interfaces
Output: allows you capture new packet file, set its size, and select a storage location for it (browse ->system name -> data). This saves captured packets in a folder called data.
Option: resolve MAC address, set how much packet to capture etcetera.

After setting option, goto Input and double click on WiFi interface to capture internet files.
These packets are automatically saved in the specified location.

2. Capture packets
A researcher should carry out the following cyber First-Aid activities in order to protect himself from malicious sites:
Double click on Wi-Fi 4 as shown in fig 4 to start capturing packets. There are 3 panels: Packet list (top), packets details (middle pane), and packet bytes (lower pane).
-Observer the top panel to see packets flow in and out of your system

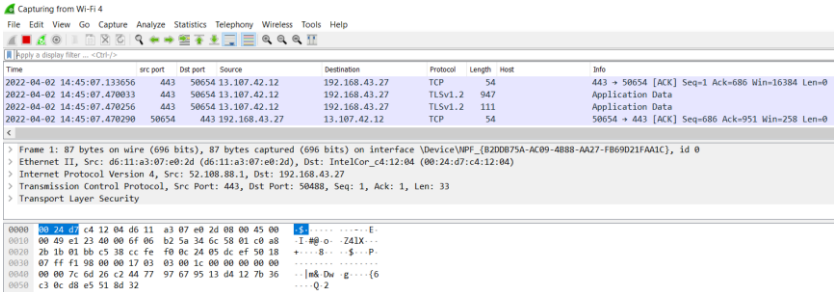


Fig.5 live packet sniffing. Source: Wireshark Screenshot

-packet type with related information is displayed in top panel example
Date and time of capture, source and destination ports, source and destination IP addresses, protocols (TCP, IP, HTTP), host name (URL) etc.
-to scan
While the researcher is on the internet, different protocols from the sites visited are captured and stored using the set parameters. The GET HTTP protocols represent the web content that are not encrypted and capturing and analyzing them can reveal malware in such applications. For encrypted sites (HTTPs), a look at TCP files Secure Socket Layer (SSL) and Transport Layer Security (TLS) and carrying out decryption action would help analyze the file (not within the context of this paper).
Most sites researchers visit are still on HTTP which is not encrypted and hence unsecure. Some examples are: foxnews.com, BBC.com, MIT.edu, Dictionary.com, NYU.edu, UN.org, FoxNews.com, Ox.ac.uk, WorldBank.org, Cornell.edu Washington.edu etcetera [34] (some of these sites are often visited by researchers for content, remote learning, collaboration or in search of grants).

3. Malware detection [33].
After online time, captured packets, downloaded files (applications, PDFs, packets, may be analyzed for malware.
-download hashmyfile.exe and save it in the folder created for packets storage (data).
-Open the location indicated for packet storage -> double click on saved packets -> apply filter.
Applying filter is for separation of the HTTP protocols you want to analyze from other protocols. Figure 6 below shoes filter names and their corresponding expressions.

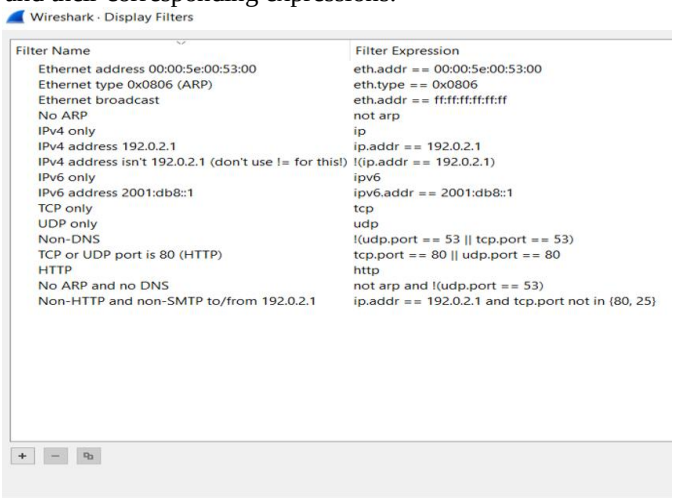


Fig.6: Filters that may be applied in Wireshark to independently monitor network traffic of interest

The result of http filter is shown in figure 7 below.

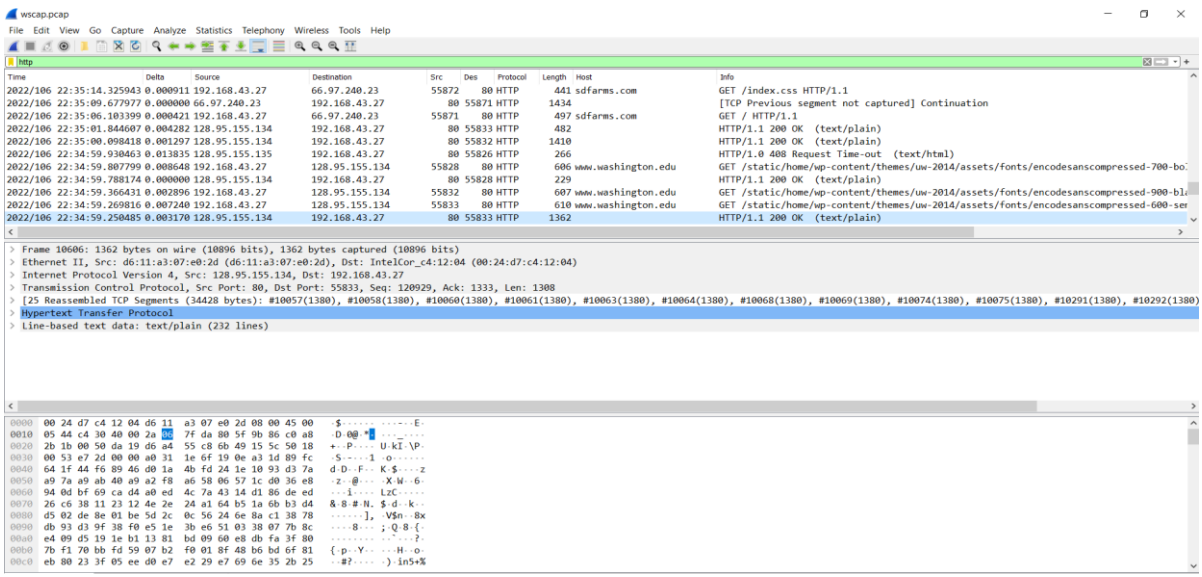


Fig.7: HTTP applications showing all information of filtered HTTP traffic.

In the address bar of opened captured data, type: http (small letters). This is called filtering as it filters all logs to display only http packets.

-To view all http captured applications, Goto File -> Export object -> HTTP -> click on content Type to sort files in alphabetical order -> select files to be investigated one after the other and with their extension names (example: java files have extension name .jar, .js for javascript files) -> save -> in the folder named "data". This is shown in figure 8 below.

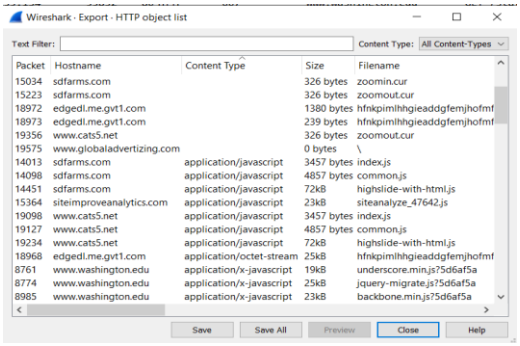
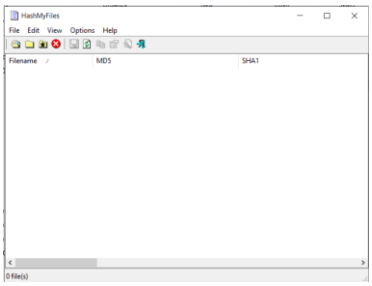


Fig.8: Exported HTTP files

-in the data folder, double click hashmyfile.exe to open, double click the open icon and select the files being investigated -> double click on the Message Digest 5 algorithm (MD5) to view editable window that can be copied for analysis. Fig. 9 and Fig. 10 show file hashing procedures while Fig.11 shows the editable window.

-open new notepad



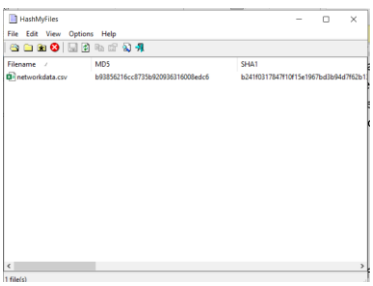


Fig.9: hash key generator without file Fig.10: Hash key generator with file

-the file name, MD5 (Message-Digest Algorithm 5) and SHA1 (Secure Hash Algorithm 1) of the suspicious file is displayed.
-Double click the file to display the details as shown in figure 10 bellow

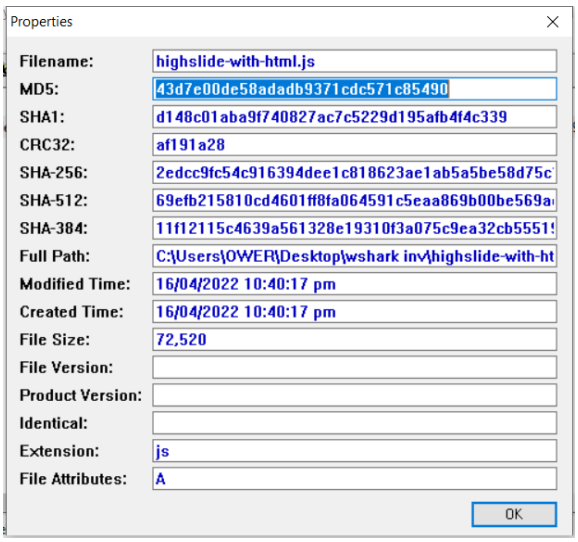


Fig.10. hash key generator output

-Check if the file is malicious
Copy the MD5 from the editable window and scan it for virus in VirusTotal online application.
-Open virustotal.com/gui/home/search
Virus Total website is a database of anti-virus vendors and blacklisted malware content. It is described as the google of malware as it matches any hash key, URL or file, entered into its search engine with what is contained in the database and returns number of vendors who flagged the content as malware content, as well as percentage of certainty rated 40 to 100; with 40 being low certainty, and 100 implying highest certainty that scanned content is malware free.
-To check if a file has malware, open Virus Total website, click on browse->goto folder where the file is located-> double-click on the file-> click on search to verify if the file has malware.
For HTTP files captured during online session, generating the file's hash key, copying the file's MD 5 (Message digest algorithm5) and scanning the MD5 using Virus Total.
For verifying URLs, before downloading any application from a website, ensure that the website is Virus free, by opening Virus Total website and type-in the URL of the website-> scan search for a malware match.
Files discovered to be compromised are removed from the researcher's computer and their sites blocked. Figure 12 is a GUI interface that has malware blacklisted by different vendors while figure 13 shows a result of virus scan.

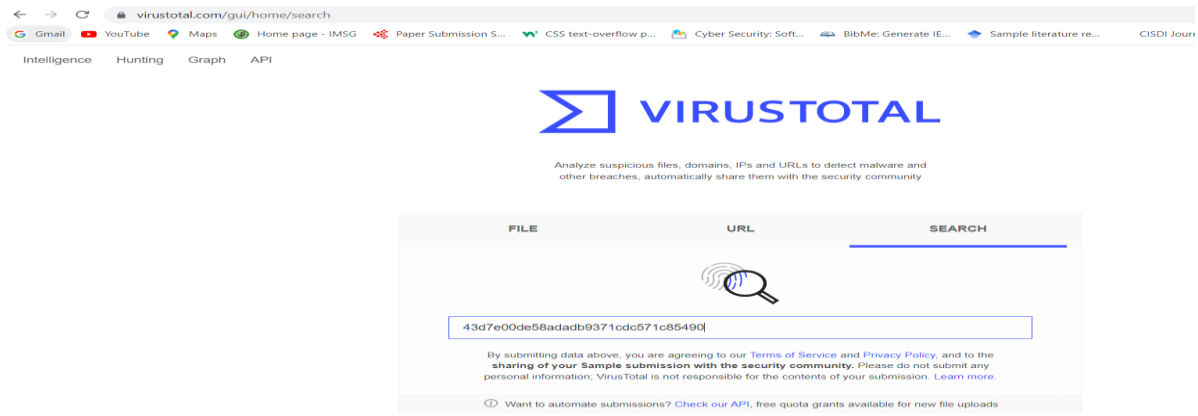


Fig.12: VirusTotal IDE for malware detection

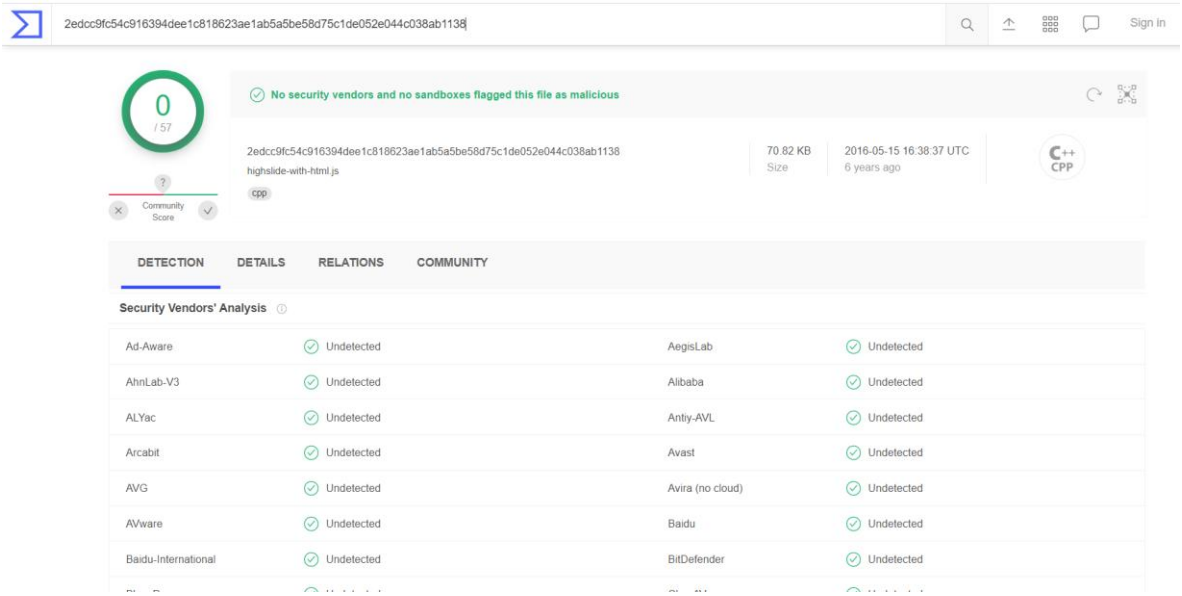


Fig. 13: Scan result of hash key shows no vendor has flagged the key as having malicious.

4. Block website malware websites

The fourth method is to block any site discovered to contain malicious content. The procedure is shown in figure14:

- Open Notepad
- Right click /run as admin/
- Goto file
- Open c:/->windows-
- ->system32 -> drivers ->etc
- Change file type from text to All files
- Enter ip address of website you want to block
- To get the ip address, ping the host name in cmd
- Eg 127.0.0.1 Facebook.com
- Save

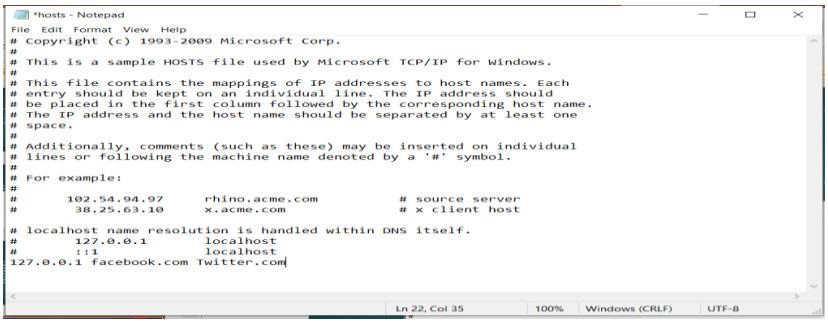


Fig.14: Notepad page example for blocking Facebook and Twitter websites

opening the blocked website shows the blocked site can no longer communicate with researchers' system (Figure 15).

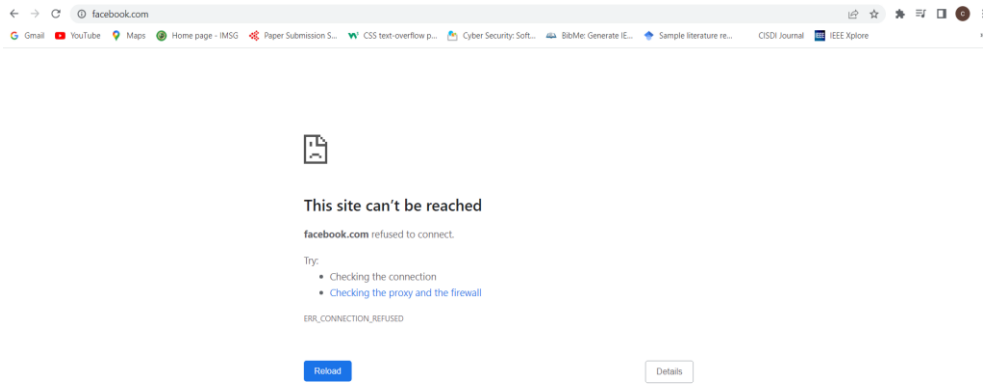


Fig. 15: Blocked site example

IV. Result

Applying cyber hygiene best-practice, monitoring, analysis and scanning of data packets, e-mail scanning, scanning of downloaded files before installing, clearing browsing cache, and blocking URL with malicious content make up cyber first-aid, and observing these methods proved effective in detection, prevention and removal of attack vectors. The first aid box and tools it contains are shown in figures 16 and 17 below:

Fig. 16: CyberFirst Aid Box

S/N	Tool	Example	Tool Application
1.	Packet Sniffers/analyzers	TCPDUMP, Wireshark https://www.wireshark.org/download.html	Computer application used to intercept network traffic, get details of dataflow, their sources and destinations as well as data items they convey.
2.	Hashing program	Hashmyfile.exe	Computer program used to extract the MAC address of applications captured by packet sniffers
3	Virustotal program	Virustotal.com/gui/home/search	Website that analyzes URL, IP addresses, files and domains to find malware and breaches
4.	Anti-Virus	Norton, Kaspersky	Software for system protection
5.	Clearing browsing history		
6.	Cyber hygiene best-practices		

Fig. 17: Tools in the cyber First Aid

V. Conclusion and Recommendations

R & D investments in recent years is evidence of its importance and growing recognition globally. Researchers work assiduously to ensure that R & D contribute meaningfully to nations' economic development. Receiving funding and grants from government and private organizations encourage collaborative research and yield higher ReturnOnInvesment (ROI). The increased interest and high investments in R & D also attract negative attention to the researcher, his on-going work, online and offline repositories, links and connections, and this has been attributed majorly, to intellectual property theft as observed by [5].

It should be noted that most sites researchers visit are still on HTTP and not HTTPs. The difference between both is that HTTPS uses a Transport Layer Security or Secured Socket Layer. There is encryption for protection of data and information in HTTPS whereas HTTP data is not secured. These include, but are not limited to: foxnews.com, BBC.com, MIT.edu, Dictionary.com, NYU.edu, UN.org, Ox.ac.uk, WorldBank.org, Cornell.edu Washington.edu, etcetera [25] (some of these sites are often visited by researchers for content, remote learning, collaboration or in search of grants).

The methods proposed in this study are readily available online and cyber security engineers are conversant with the malware detection methods. The contribution of this study however, is to devise a new application of knowledge by presenting easy-to-use cyber security practices that researchers from every research field can learn and adopt. This work also creates situational awareness of the need for all researchers to have basic knowledge of malware scanning, detection, and containment, as a cyber first-aid.

It is recommended therefore, that:

1. Researchers engage in basic cyber hygiene practices such as:
   -Having up-to-date antivirus installed
   -Ensuring the system firewall is on
   -Scanning the computer with active antivirus from time to time
   -Verifying publishers before downloading from them
   -Not opening e-mails from unknown sources
   -Backing-up files to the cloud is also recommended
   -Malware antivirus for USB devices,
   -Updating applications and systems software,
   -Changing passwords from time-to-time
2. Clear browser cache
3. Sniff and analyze packets, scan the packet data, PDFs, e-mails, URLs, and other downloaded applications for Malicious content when visiting or downloading from sites not quite secure and verify if downloaded file contains malware and block its websites to avoid further communication.
4. Block sites discovered to contain malware.

References

[1] C. Bloch and M. P. Sørensen, "The size of research funding: Trends and implications," *Sci. Public Policy*, vol. 42, no. 1, pp. 30–43, Feb. 2015, doi: 10.1093/SCIPOL/SCU019.

[2] B. Ebersberger, "The Impact of Public R&D Funding," *VTT Publ.*, 2005.

[3] A. M. Diego Ubfal, "The Impact of Funding on Research Collaboration: Evidence from Argentina | Publications." https://publications.iadb.org/publications/english/document/The-Impact-of-Funding-on-Research-Collaboration-Evidence-from-Argentina.pdf (accessed Mar. 29, 2022).

[4] J. Sussex *et al.*, "Quantifying the economic impact of government and charity funding of medical research on private research and development funding in the United Kingdom," *BMC Med.*, vol. 14, no. 1, 2016, doi: 10.1186/s12916-016-0564-z.

[5] E. Ukwandu *et al.*, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," no. March, 2021, doi: 10.3390/info13030146.

[6] "(2) (PDF) Revisiting Cyber Definition." https://www.researchgate.net/publication/334989724_Revisiting_Cyber_Definition (accessed Apr. 04, 2022).

[7] "cyberspace - Glossary | CSRC." https://csrc.nist.gov/glossary/term/cyberspace (accessed Apr. 04, 2022).

[8] "Cyber Attack - Glossary | CSRC." https://csrc.nist.gov/glossary/term/cyber_attack (accessed Apr. 04, 2022).

[9] "What is Cyber Security? | Definition, Types, and User Protection." https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security (accessed Apr. 04, 2022).

[10] "15 Cybersecurity in Education Stats You Should Know for 2020." https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/ (accessed Apr. 04, 2022).

[11] "Difference between Network and Internet." https://www.guru99.com/difference-between-network-and-internet.html (accessed Apr. 01, 2022).

[12] X. Jing, Z. Yan, and W. Pedrycz, "Security data collection and data analytics in the internet: A survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 586–618, Jan. 2019, doi: 10.1109/COMST.2018.2863942.

[13] "What is a packet? | Network packet definition | Cloudflare." https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-packet/ (accessed Apr. 01, 2022).

[14] Baset Mohamad, "Machine Learning for Malware Detection," *Msc Proj.*, no. November, pp. 1–17, 2016.

[15] E. Özeri and M. İskefiyel, "Detection of DDoS attack via deep packet analysis in real time systems," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, pp. 1137–1140, Oct. 2017, doi: 10.1109/UBMK.2017.8093526.

[16] H. ur Rahman, G. Wang, M. Z. A. Bhuiyan, and J. Chen, *Towards In-Network Generalized Trustworthy Data Collection for Trustworthy Cyber-Physical Systems*, vol. 1123 CCIS, no. November. Springer Singapore, 2019.

[17] V. K. Tiwari and R. Dwivedi, "Analysis of cyber attack vectors," *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016*, no. February, pp. 600–604, 2017, doi: 10.1109/CCAA.2016.7813791.

[18] V. G. Cerf and R. E. Kahn, "A Protocol for Packet Network Intercommunication," *IEEE Trans. Commun.*, vol. 22, no. 5, pp. 637–648, 1974, doi: 10.1109/TCOM.1974.1092259.

[19] I. Ahmed and K. suk Lhee, "Classification of packet contents for malware detection," *J. Comput. Virol.*, vol. 7, no. 4, pp. 279–295, 2011, doi: 10.1007/s11416-011-0156-6.

[20] N. S. Selamat and F. H. M. Ali, "Comparison of malware detection techniques using machine learning algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 1, pp. 435–440, 2019, doi: 10.11591/ijeecs.v16.i1.pp435-440.

[21] R. Cheng and G. Watson, "D 2 PI : Identifying Malware through Deep Packet Inspection with Deep Learning," 2018.

[22] J. C. Kimmell, M. Abdelsalam, and M. Gupta, "Analyzing Machine Learning Approaches for Online Malware Detection in Cloud," *Proc. - 2021 IEEE Int. Conf. Smart Comput. SMARTCOMP 2021*, no. Ml, pp. 189–196, 2021, doi: 10.1109/SMARTCOMP52413.2021.00046.

[23] A. Corum, D. Jenkins, and J. Zheng, "Robust PDF Malware Detection with Image Visualization and Processing Techniques," *Proc. - 2019 2nd Int. Conf. Data Intell. Secur. ICDIS 2019*, pp. 108–114, 2019, doi: 10.1109/ICDIS.2019.00024.

[24] P. Prasse, G. Gruben, T. Pevny, M. Sofka, and T. Scheffer, "Malware Detection by HTTPS Traffic Analysis," *Math. Fak. Potsdam Univ.*, 2017.

[25] E. Özeri and M. İskefiyel, "Detection of DDoS attack via deep packet analysis in real time systems," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, no. October 2017, pp. 1137–1140, 2017, doi: 10.1109/UBMK.2017.8093526.

[26] D. Bekerman, B. Shapira, L. Rokach, and A. Bar, "Unknown malware detection using network traffic classification," *2015 IEEE Conf. Commun. NetworkSecurity, CNS 2015*, pp. 134–142, Dec. 2015, doi: 10.1109/CNS.2015.7346821.

[27] M. Sikorski and A. Honig, "Hashing: A Fingerprint for Malware - Practical Malware Analysis [Book]." https://www.oreilly.com/library/view/practical-malware-analysis/9781593272906/ch02s02.html (accessed Apr. 03, 2022).

[28] T. Roccia, "Fifty Shades of Malware Hashing. In forensic investigation as well as… | by Thomas Roccia | SecurityBreak |

Medium." https://medium.com/malware-buddy/fifty-shades-of-malware-hashing-3783d98df59c (accessed Apr. 03, 2022).
[29] I. Ghafir and V. Prenosil, "Malicious file hash detection and drive-by download attacks," *Adv. Intell. Syst. Comput.*, vol. 379, no. September, pp. 661–668, 2016, doi: 10.1007/978-81-322-2517-1_63.
[30] L. Stosic and D. Velickovic, "Computer security and security technologies," *J. Process Manag. New Technol.*, vol. 1, no. 1, pp. 14–19, 2013, doi: 10.5937/JPMNT1301014S.
[31] B. De Decker, "Introduction to computer security," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1528, pp. 377–393, 1998, doi: 10.1007/3-540-49248-8_19.
[32] "Wireshark · Download." https://www.wireshark.org/download.html (accessed Apr. 03, 2022).
[33] "Wireshark - Malware traffic Analysis - YouTube." https://www.youtube.com/watch?v=3t1BNAavrlQ (accessed Mar. 29, 2022).
[34] "For shame: You'll never believe the sites still on HTTP - Android Authority." https://www.androidauthority.com/sites-still-on-http-889265/ (accessed Apr. 04, 2022).

Cyber First-Aid, et. al. "XXXXXXXXXXXXXXXXXX." *IOSR Journal of Mobile Computing & Application (IOSR-JMCA)*, *9*(3), (2022): pp. 01-12.